MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR

DEPARTMENT OPERATING REGULATION NUMBER
DOR 8.350

CHAPTER	SUBCHAPTER	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Regulatory Compliance	HIPAA Regulations	4-15-2013	4	1 of 4

Subject	AUTHORITY	History – see below
Information Security Incidents	630.050 RSMo	

PERSON RESPONSIBLE	SUNSET DATE
Chief Security Officer	7-1-2016

PURPOSE: The policy of the Missouri Department of Mental Health (DMH) is to secure consumer's protected health information in compliance with federal law and federal regulations at 45 CFR Parts 160, 162, 164 and 42 CFR Part 2. This DOR establishes the normal day-to-day security activity and outlines what steps shall be taken in the event of an information security incident.

APPLICATION: Applies to DMH, its facilities and workforce.

(1) DEFINITIONS

(A) Computer Systems – Computers connected to local and statewide communication networks, database storage or electronic records systems, Internet or email or other DMH computing devices such as PDA's or stand-alone PC's.

(B) DMH Workforce –Includes all state employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity (facility or DMH). This shall include client workers employed by DMH or its facilities.

(C) Chief Security Officer (CSO) – Individual designated to oversee all activities related to the development, implementation, maintenance of, and adherence to DMH and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

(D) Local Security Officer (LSO) – Individual designated to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer.

(E) Security Incident – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(F) Information Security Management Office (ISMO) –The unit at the State of Missouri's Office of Administration responsible for monitoring the State of Missouri Computer network and notifying agencies of the State of Missouri's threat level.

(G) Electronic Protected Health Information (E-PHI) – Individually identifiable health information that is transmitted or maintained in electronic media or transmitted or maintained in any other form or medium.

(2) A security incident can take many forms. The DMH Workforce should be aware of their role in securing DMH data and report any of the following possible security events if observed:

a. Improper use of staff access privileges both of a physical and technical nature;
b. Staff accessing data to damage or steal information;
c. Physical breach to building or locked areas;
d. Changes to system hardware, software or suspicious activity on staff workstations;
e. Loss of paper or electronic data (laptop or other device stolen, paper file lost or misplaced); or
f. Data disseminated to improper recipients (a consumer's electronic protected health information sent somewhere without a need to know).

(3) Security Incident Handling

a. Any suspected activity should be immediately reported to the facility LSO who shall initiate an ITSD help ticket using the category "Event/Incident Analysis". If the LSO is not available, staff should contact the ITSD Help Desk who will initiate a help ticket using the category listed above. This ticket category will be routed directly to ISMO who will begin an investigation of the event. The CSO should also be informed.
b. The initiation of the ITSD Help Desk ticket will engage the ISMO to begin an investigation using the Missouri Information Security Incident Response Plan.
c. The ISMO will coordinate with the DMH CSO and any other DMH or ITSD staff necessary to conduct a thorough investigation.
d. If, after initial research, the ISMO believes a breach of sensitive information may have occurred, DMH will activate the breach DOR to determine if further action is needed.

(4) Documentation

a. The LSO will complete the Report of Security Incident form, attached to this DOR, within 30 (thirty) days. The form shall be kept for six (6) years.
b. Any disclosures of consumer protected health data shall be documented in the disclosure database by the LSO. The database can be accessed from dmhonline, Applications, Disclosures.

(5) There shall be no facility policies pertaining to this topic. DMH Operating Regulations shall control.

(6) Sanctions. Failure of workforce members to comply or ensure compliance with the DOR may result in disciplinary action, up to and including dismissal.

(7) Review Process. The CSO may collect summaries of security incidents from each facility during the month of April each year for the purpose of analyzing trends and issues associated with compliance of this regulation.

HISTORY: Original DOR effective September 1, 2004. On July 1, 2008 the sunset date was extended to July 1, 2011. Amendment effective July 1, 2008. On June 29, 2011 the sunset date was extended to July 1, 2014. Amendment effective June 29, 2011. Amendment effective April 15, 2013.

	Missouri Department of Mental Health Information Technology **Report of Security Incident** Facility Name _____	**Local Security Officer Use Only:** Local Security Officer Signature: _____ Received Date: _____

I. Instructions: *This form shall be used to report any acts or omissions that result in (1) the attempted or successful unauthorized access, use, disclosure, modification or destruction of information; or (2) interference with system operations in an information system.*

II. Type of Incident	**III. Date & Time of Incident**
IV. System Compromised/Damage Caused	
V. Employee(s) Involved:	
VI. Initial Action Taken:	**VII. Remedy Implemented:**
VIII. Remedy Date:	
IX. Date Reported to Local Security Officer:	
X. Person Reporting: _____ Work Location: _____ *Signature*	
When completed, please send to the Local Security Officer for further investigation and actions if necessary.	
SECTION BELOW FOR USE BY LOCAL SECURITY OFFICER	
XI. FOLLOW UP ACTION BY LSO:	
XII: Date Reported to Superintendent:	
XII. Date Reported to HIPAA Privacy Officer:	
XIV. Local Security Officer Signature: _____	
Documentation of investigation by Local Security Officer should be attached.	
SECTION BELOW FOR USE BY HUMAN RESOURCES	
XV. Personnel Action Taken (Punitive, Probationary or Written plan of Probation):	**XVI. Date Personnel Action Taken:**